In the Claims:

1.   (Previously Presented) A method for maintaining network activity data for an intrusion detection system, comprising:

storing data representative of network activity in datasets, the datasets including root datasets each having a root keyset and child datasets each having a child keyset with a key combination being a subset of, and less granular than, a root keyset; and

identifying a child dataset of a root dataset through the root dataset.

2.   (Original) The method of Claim 1, further comprising identifying a plurality of child datasets of the root dataset through the root dataset.

3.   (Original) The method of Claim 1, further comprising identifying all child datasets of the root dataset through the root dataset.

4.   (Original) The method of Claim 1, further comprising identifying the child dataset of the root dataset with a pointer from the root dataset to the child dataset.

5.   (Original) The method of Claim 1, further comprising identifying all child datasets through their root datasets.

6.   (Original) The method of Claim 1, wherein each root dataset comprises a plurality of child datasets.

7.   (Original) The method of Claim 1, wherein the root dataset includes a sibling root dataset, the sibling root dataset and the root dataset having root keysets a reverse of each other, further comprising identifying the sibling root dataset through the root dataset.

8.   (Original) The method of Claim 7, wherein the root dataset and the sibling root dataset collectively identify all of their child datasets and identify one another.

9.   (Original) The method of Claim 1, wherein the root keysets each comprise a source address key and a destination address key.

10.   (Original) The method of Claim 1, wherein the root keysets comprise quad keysets.

11.   (Original) The method of Claim 10, wherein the quad keysets each comprise a source address key, a source port key, a destination address key and a destination port key.

12.   (Original) The method of Claim 1, wherein the child keysets comprise one of single, dual and triple keysets.

13.   (Original) The method of Claim 1, wherein the root keysets comprise stream based keysets.

14.   (Original) The method of Claim 13, wherein the stream based keysets comprise a source address key, a source port key, a destination address key and a destination port key, a first child keyset comprises a source address key and a destination address key, a second child keyset comprises a destination address key and a destination port key, and a third child keyset comprises a source address key and a destination port key.

15.   (Original) The method of Claim 1, wherein the datasets comprise data buckets.

16.   (Original) The method of Claim 1, further comprising identifying all child datasets of the root dataset through the root dataset with a single search of a database storing the datasets.

17.   (Original) The method of Claim 1, further comprising:
receiving a traffic signature not having a root dataset;
generating a root dataset having a root keyset representative of the traffic signature;
identifying all existing child and sibling root datasets of the root dataset;

generating all absent child and sibling root datasets of the root dataset; and

associating the child and sibling root datasets with the root dataset.

18.   (Original) The method of Claim 1, further comprising automatically removing outdated root datasets and child datasets.

19.   (Original) The method of Claim 18, further comprising storing a counter for each child dataset, the counter operable to indicate an outdated status of the child dataset.

20.   (Original) The method of Claim 1, further comprising retrieving data for processing a traffic signature by searching a data storage system including the datasets for an existing root dataset having a root keyset corresponding to the traffic signature and identifying all child datasets, sibling root datasets, and child datasets of the sibling root datasets through the root dataset.

21.   (Currently Amended) An intrusion detection system, comprising:

logic encoded in computer-readable media; and

the logic operable to store data representative of network activity in datasets, the datasets including root datasets each having a root keyset and child datasets each having a child keyset with a key combination being a subset of, and less granular than, a root keyset and further operable to identify a child dataset for a root dataset through the root dataset.

22.   (Original) The intrusion detection system of Claim 21, the logic further operable to identify a plurality of child datasets of the root dataset through the root dataset.

23.   (Original) The intrusion detection system of Claim 21, the logic further operable to identify all child datasets of the root dataset through the root dataset.

24.   (Original) The intrusion detection system of Claim 21, the logic further operable to identify the child dataset of the root dataset with a pointer from the root dataset to the child dataset.

25.   (Original)   The intrusion detection system of Claim 21, the logic further operable to identify all child datasets through their root datasets.

26.   (Original)   The intrusion detection system of Claim 21, wherein each root dataset comprises a plurality of child datasets.

27.   (Original)   The intrusion detection system of Claim 21, wherein the root dataset includes a sibling root dataset, the root dataset and the sibling root dataset having root keysets a reverse of each other, the logic further operable to identify the sibling root dataset through the root dataset.

28.   (Original)   The intrusion detection system of Claim 27, wherein the root dataset and the sibling root dataset collectively identify all of their child datasets and identify one another.

29.   (Original)   The intrusion detection system of Claim 21, wherein the root keysets each comprise a source address key and a destination address key.

30.   (Original)   The intrusion detection system of Claim 21, wherein the root keysets comprise quad keysets.

31.   (Original)   The intrusion detection system of Claim 30, wherein the root keysets comprise quad keysets, the quad keysets each including a source address key, a source port key, a destination address key, and a destination port key.

32.   (Original)   The intrusion detection system of Claim 21, wherein the child keysets comprise one of single, dual and triple keysets.

33.   (Original)   The intrusion detection system of Claim 21, wherein the root keysets comprise stream based keysets.

34.   (Original)   The intrusion detection system of Claim 21, the logic further operable to receive a traffic signature not having a root dataset, to generate a root dataset having a root keyset representative of the traffic signature, to identify all existing child and sibling root datasets of the root dataset, to generate absent child and sibling root datasets of the root dataset and to associate the child and sibling root datasets of the root dataset with the root dataset.

35.   (Original)   The intrusion detection system of Claim 21, wherein the datasets comprise data buckets.

36.   (Original)   The intrusion detection system of Claim 21, the logic further operable to automatically remove outdated root and child datasets.

37.   (Original)   The intrusion detection system of Claim 36, the logic further operable to maintain a counter for each child dataset, the counter operable to indicate an outdated status of the child dataset.

38.   (Original)   The intrusion detection system of Claim 21, the logic further operable to retrieve data for processing of a traffic signature by searching a data storage system including the datasets for an existing root dataset corresponding to the traffic signature and to identify all child datasets, sibling root datasets and child datasets of the root dataset and the sibling root dataset through the root dataset.

39.   (Previously Presented) A system for maintaining data on network activity for an intrusion detection system, comprising:

means for storing data representative of network activity in datasets, the datasets including root datasets each having a root keyset and child datasets each having a child keyset with a key combination being a subset of, and less granular than, a root keyset; and

means for identifying a child dataset of a root dataset through the root dataset.

40.   (Original) The system of Claim 39, further comprising means for identifying the child dataset of the root dataset with a pointer from the root dataset to the child dataset.

41.   (Original) The system of Claim 39, further comprising means for identifying all child datasets of the root dataset through the root dataset.

42.   (Original) The system of Claim 39, further comprising means for identifying all child datasets through their root datasets.

43.   (Original) The system of Claim 39, wherein the root datasets include a sibling root dataset, the sibling root dataset and the root dataset having root keysets a reverse of each other, further comprising means for identifying the root dataset and the sibling root dataset through each other.

44.   (Original) The system of Claim 39, further comprising:

means for receiving a traffic signature not having a root dataset;

means for generating a root dataset having a root keyset representative of the traffic signature;

means for identifying all existing child and sibling root datasets of the root dataset;

means for generating absent child and sibling root datasets of the root dataset; and

means for associating the child and sibling root datasets of the root dataset with the root dataset.

45.   (Original)   The system of Claim 39, further comprising means for automatically removing outdated root datasets and child datasets.

46.   (Original) The system of Claim 39, further comprising:

means for retrieving data for processing of a traffic signature by searching a data storage system for an existing root dataset having a root keyset corresponding to the traffic signature; and

means for identifying all child datasets, sibling root datasets, and child datasets of the root dataset through the root dataset.

47.   (Cancelled)

48.   (Cancelled)

49.   (Cancelled)

50.   (Original) A method for maintaining data on Internet Protocol (IP) traffic for an intrusion detection system, comprising:

storing data representative of network activity in datasets, the datasets including root datasets each having a quad keyset comprising a source address key, a source port key, a destination address key and a destination port key and child datasets each having a dual keyset with a key combination derived from and less granular than a quad keyset of a root dataset;

storing pointers for each root dataset, the pointers each identifying a child dataset having a dual keyset derived from the quad keyset of the root dataset and a sibling root dataset having a quad keyset a reverse of the quad keyset of the root dataset; and

retrieving data for processing of a traffic signature by performing a single search for a root dataset having a quad keyset corresponding to the traffic signature and identifying relevant child and sibling root datasets through the pointers of the root dataset.

51.   (Original) The method of Claim 50, wherein the dual keysets include a first dual keyset comprising a source address key and a destination address key, a second dual keyset comprising a destination address key and a destination port key, and a third dual keyset comprising a source address key and a destination port key.

52.   (Previously Presented) A method for maintaining network activity data for an intrusion detection system, comprising:

storing data representative of network activity in datasets, the datasets including root datasets each having a root keyset and child datasets each having a child keyset with a key combination derived from and less granular than a root keyset;

identifying a child dataset of a root dataset through the root dataset;

receiving a traffic signature not having a root dataset;

generating a root dataset having a root keyset representative of the traffic signature;

identifying all existing child and sibling root datasets of the root dataset;

generating all absent child and sibling root datasets of the root dataset; and

associating the child and sibling root datasets with the root dataset.

53.   (Previously Presented) A method for maintaining network activity data for an intrusion detection system, comprising:

storing data representative of network activity in datasets, the datasets including root datasets each having a root keyset and child datasets each having a child keyset with a key combination derived from and less granular than a root keyset;

identifying a child dataset of a root dataset through the root dataset; and

retrieving data for processing a traffic signature by searching a data storage system including the datasets for an existing root dataset having a root keyset corresponding to the traffic signature and identifying all child datasets, sibling root datasets, and child datasets of the sibling root datasets through the root dataset.

54.   (Currently Amended) An intrusion detection system, comprising:

logic encoded in computer-readable media;

the logic operable to store data representative of network activity in datasets, the datasets including root datasets each having a root keyset and child datasets each having a child keyset with a key combination derived from and less granular than a root keyset and further operable to identify a child dataset for a root dataset through the root dataset; and

the logic further operable to retrieve data for processing of a traffic signature by searching a data storage system including the datasets for an existing root dataset corresponding to the traffic signature and to identify all child datasets, sibling root datasets and child datasets of the root dataset and the sibling root dataset through the root dataset.

55.   (Previously Presented) A system for maintaining data on network activity for an intrusion detection system, comprising:

means for storing data representative of network activity in datasets, the datasets including root datasets each having a root keyset and child datasets each having a child keyset with a key combination derived from and less granular than a root keyset;

means for identifying a child dataset of a root dataset through the root dataset;

means for receiving a traffic signature not having a root dataset;

means for generating a root dataset having a root keyset representative of the traffic signature;

means for identifying all existing child and sibling root datasets of the root dataset;

means for generating absent child and sibling root datasets of the root dataset; and

means for associating the child and sibling root datasets of the root dataset with the root dataset.

56.   (Previously Presented) A system for maintaining data on network activity for an intrusion detection system, comprising:

means for storing data representative of network activity in datasets, the datasets including root datasets each having a root keyset and child datasets each having a child keyset with a key combination derived from and less granular than a root keyset;

means for identifying a child dataset of a root dataset through the root dataset;

means for retrieving data for processing of a traffic signature by searching a data storage system for an existing root dataset having a root keyset corresponding to the traffic signature; and

means for identifying all child datasets, sibling root datasets, and child datasets of the root dataset through the root dataset.